⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭60－136440

⑤1Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　昭和60年(1985)7月19日
H 04 L 9/02　Z－7240－5K

審査請求 有　発明の数 1　(全11頁)

⑤4発明の名称　セッション暗号キー更新方法

⑳特　願　昭59－243557
㉒出　願　昭59(1984)11月20日
優先権主張　㉜1983年12月21日㉝イギリス(GB)㉛83307786.0

⑦2発　明　者　クリストファー・ホラウエイ　イギリス国エヌダブリュー2、1アール・デイ、ロンドン、クリツクルウツド、ソーヴアントン・ロード、ソーヴアントン・コート1番地
⑦1出　願　人　インターナショナル・ビジネス・マシーンズ・コーポレーション　アメリカ合衆国10504、ニユーヨーク州アーモンク（番地なし）
⑦4代　理　人　弁理士　頓宮　孝一　外1名

## 明　細　書

1.発明の名称　セッション暗号キー更新方法

2.特許請求の範囲

ホストデータプロセッサが通信ネットワークを介して各々検証モジユールを含む複数のメッセージ起点ユニットに接続され、各検証モジュールごとに取引きセッションキーを発行し記憶し、ユーザの入力装置で記憶されるユーザ識別番号と、ユーザが別に記憶している秘密番号と、から導出されるユーザ確認パラメータを各ユーザごとに発行し記憶するようなデータ通信システムにおいて、

(a) ユーザによつて取引きがメッセージ起点ユニットで開始されると、検証モジユールがユーザ識別番号と、現取引きセッションキーに基づくメッセージ確認コードと、を含む第1のメッセージを形成してホストデータプロセッサへ送るステップと、

(b) ホストデータプロセッサで第1のメッセージを受け取つてメッセージ確認コードを再生成し、これと受信したメッセージ確認コードとを比較するステップと、

(c) ランダムキーを生成するステップと、

(d) ランダムキー、ユーザ確認パラメータ、および現取引きセッションキーに基づき新たな取引きセッションキーを生成するステップと、

(e) 現取引きセッションキーを用いて暗号化されたユーザ確認パラメータと、ユーザ確認パラメータを用いて暗号化されたランダムキーと、を含む第2のメッセージを形成して検証モジユールへ送るステップと、

(f) 検証モジユールでユーザの入力する秘密番号を受け取つてユーザ確認パラメータを再生成するステップと、

(g) 再生成されたユーザ確認パラメータと受信したユーザ確認パラメータとを比較してユーザの入力を検証し、これにより検証された正しいユーザ確認パラメータを用いてランダムキーを暗号解読し、ホストデータプロセッサに送られる次のメッセージのために使用される新たな取引きセッショ

ンキーを生成し記憶するステップと、

を有することを特徴とするセッション暗号キー更新方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明はデータ通信システムの安全保護の技術に関する。

〔従来技術〕

金融取引きに関するメッセージを伝えるデータ通信ネットワークは今日では広く一般に使用されるようになつた。磁気ストライプカードと秘密番号（ＰＩＮ）を有する銀行の顧客によつて操作され、遠隔のデータ処理機械にオンラインで接続される現金支払端末機は今やどくあたりまえのものとなつている。さらに、単に現金を支払うだけでなくより多くの機能を遂行することのできる自動現金預払機（ＡＴＭ）が登場し、金融取引きに関わる大量のペーパーワーク（小切手の処理など）



を減じねばならないという経済的な要求に答えている。

小売業者がパケット交換網に接続された端末を有し、顧客が買物をしたときに借方の記入された勘定書を小売業者の端末からオンラインで受け取るようなＰＯＳ／ＥＦＴ（Point of sale/electronic funds transfer）システムもまた開発されている。

英国特許出願第８３２４９１６号にはＰＯＳ／ＥＦＴシステムに関する記載がある。この特許出願にはさらにユーザおよびメッセージ確認検査用のシステムに関する記載もある。これらのシステムでは、店に設置された小売業者の端末が、公衆交換通信システムを介して、カード発行サービス機関のデータ処理センターに接続されるようなＥＦＴシステムが記載されている。そのシステムのユーザには機密保持されたバンクカードが発行される。このカードはマイクロプロセッサ、ＲＯＳ、およびＲＡＭを有する。カードの発行業者がカードをユーザに発行する際、そのカードのＲＯＳに



個人キー（ＫＰ）と会計番号（ＰＡＮ）を記憶する。ユーザも個人識別番号（ＰＩＮ）を有しそれを個人個人で覚えておく。

小売業者の端末に接続されたＥＦＴモジュールにカードを入れると、取引が開始される。そうしてＰＡＮおよびセッションキー（ＫＳ）を含む要求メッセージがカード発行業者のデータ処理センターに送られる。カード発行業者は自身の記憶するＫＰおよびＰＩＮのバージョンならびに端末から受信した時間経過パラメータに基づいて確認パラメータ（ＴＡＰ）を生成する。ＴＡＰは応答メッセージで端末に戻される。入力されたＰＩＮに基づき、カードに入つているＰＩＮおよびＫＰを部分的に処理することによつて得られたＴＡＰと、端末に戻つてきたＴＡＰを比較する。両者が一致すればそれは入力されたＰＩＮが有効であることを意味する。

要求メッセージはＫＳの下でコード化されたＰＡＮと定義域間キーの下でコード化されたＫＳを含む。メッセージ確認コード（ＭＡＣ）が各メッ



セージに付加される。ＫＳの下でコード化された項を含むメッセージにより受信されたＭＡＣと再生されたＭＡＣとで、受信されたＫＳが有効であることと、そのメッセージが有効な端末またはカードから発せられたものであることを示す。

ＥＦＴシステムには下記に示す幾つかの従来技術がある。

欧州特許公開第３２１９３号はユーザおよび小売業者が、各々、暗号キー（小売業者のキー：Kr、ユーザのキー：Kp）を有し、この暗号キーがユーザの会計番号および小売業者の業務番号と共にホストＣＰＵのデータ記憶装置に記憶されるようなシステムについて記載するものである。小売業者のキーＫｒおよびユーザのキーＫｐは、小売業者の取引用端末とホストＣＰＵとの間で送られるデータを暗号化する際に用いられる。もちろん、ホストＣＰＵに識別番号と暗号キーを有するユーザだけがこのシステムを利用できることは言うまでもない。しかしながらユーザの数が増えてくると、対応するキーおよび識別番号の検索に要する時間

はオンライン取引き処理には到底容認できないようなものになる。しかもこのシステムは単一の定義域だけであり、個人識別番号（ＰＩＮ）を使用しない。ユーザの識別の検証はホスト側で行われ、かつ、ＰＩＮを用いないので、盗用されたカードが使用されてもこれを防ぐ手だてがない。

欧州特許公開第１８１２９号は通信路上のデータの安全保護を図る方法について記載するものである。ユーザ識別コードまたは端末識別コードを主暗号キーと共に用いて、ダイヤル呼出し式データ通信ネットワークの守秘権および安全保護が提供される。有効な識別コードと主暗号キーとを対にしたもののリストがＣＰＵに保持されている。ＣＰＵへ送られた識別コードと暗号キーの対はＣＰＵに記憶されているコード対と比較される。両者が一致すればＣＰＵは端末から送られてきたコード化されたデータを受諾する。ネットワークを介して送られる全てのデータは関係したユーザキーまたは端末キーを用いて暗号化され、許可されないアクセスは予防される。このシステムも単一



定義域であり、全ての端末キー（またはユーザキー）は中央ホスト側で認識しなければならない。この特許公開は多重ホスト環境について言及するものではない（交換問題について言及しない）。

英国特許出願第２０５２５１３Ａ号はネットワーク（たとえば前記２つの欧州特許公開に示されるネットワーク）において局ごとに明らかな個人識別番号（ＰＩＮ）のようなユーザ識別情報を伝送する必要をなくした装置および方法が記載されている。ＰＩＮはユーザ局でランダムに生成された番号を用いてコード化され、ランダムに生成された番号およびコード化されたＰＩＮは処理局に送られる。処理局では、受信したこれらのランダム番号およびコード化されたＰＩＮを用いて、一般的に適用できる第２のＰＩＮがコード化され、この第２のＰＩＮと受信したＰＩＮとの比較により、受信したＰＩＮの有効性が判断される。このシステムは個人キーを使用しないので、これを十分に機密保持された安全保護システムにしようとすると、少なくとも１４個のランダム文字（各々



４ビット）を有するＰＩＮが必要になつてくる。これは人間工学上は不利なものとなる。というのは、ユーザがそのような長い文字列を覚えておかねばならないのは面倒なことであるし、また文字列が長いためにそれを誤つて入力してしまう確率も高くなるからである。ランダムな文字列は覚えにくいというので、ユーザが記憶し易いような文句をＰＩＮとして用いるとすれば、そのような文句は２８文字程度は必要である。したがつて、情報の記憶の問題がなくなつたとしても、依然として長い文字列の入力という人間工学上の問題は残る。

これまでに説明したシステムによつて可能となるＥＦＴシステムは全てのユーザ（小売業者と顧客の両方）の勘定台を保持するのは単一のホストＣＰＵに限られている。

ところで多くのカード発行機関（銀行、クレジットカード会社等）が接続され、かつ電話交換機のような交換網を介して何百もの小売業者が接続されるＥＦＴシステムは安全保護上多くの問題が



ある。

国際公開ＷＯ８１／０２６５５号はエントリー端末でＰＩＮの暗号化が２回以上行われるような多重ホスト、多重ユーザシステムについて記憶するものである。取引きの検証および許可に必要なデータがホストコンピュータに送られて、ホストコンピュータは暗号の解読に必要なデータを自身の記憶するデータベースからアクセスし、暗号化されたＰＩＮを含む取引きを検証する。秘密の端末マスターキーは各端末で保管されねばならない。これらのマスターキーのリストはホストコンピュータ側にも保管されている。

カード発行機関の各ホストコンピュータで端末マスターキーのリストを保管するのは複雑なシステム（カード発行ホストで端末キーが管理されない、したがつて、カード発行ホストで端末キーがわからないようなシステム）においては明らかに困難な作業である。

欧州特許公開第５５５８０号はエントリー点である端末でＰＩＮの検証を行うことによつてネッ

トワークにおけるＰＩＮ情報の伝送の必要性をなくそうと意図するものである。これは銀行識別子（ＢＩＮ）、ユーザの会計番号（ＡＣＣＮ）、およびＰＩＮオフセット番号が磁気ストライプにコード化されたカードを各ユーザに発行することによつて達成される。ＰＩＮ、ＢＩＮ、およびＡＣＣＮからＰＩＮオフセットが計算される。ユーザは端末に接続されたキーボードからＰＩＮを入れる。端末はカードからもＰＩＮオフセット、ＢＩＮ、およびＡＣＣＮを読み取る。そうして端末はＢＩＮ、ＡＣＣＮ、およびユーザの入れたＰＩＮからＰＩＮオフセットを再び計算する。この再計算されたＰＩＮオフセットがカードから読み取られたＰＩＮオフセットと同じなら、そのＰＩＮは正しいと推定される。この手法はそのシステムが認証に関与しないという欠点と、ＰＩＮオフセットがＰＩＮ、ＢＩＮ、およびＡＣＣＮから計算されるとわかれば、そのからくりを知つたものなら有効なＰＩＮを有する不正なカードを作ることができてしまうという欠点がある。

（11）

マイクロ回路チップ技術の発展により、今や、ユーザカードはユーザデータを磁気ストライプに記憶する代わりに、ＲＯＳを備えたマイクロプロセッサを包含できるようになつた。マイクロプロセッサはカードをＥＦＴ端末に入れたときに活動化され、適切な電力供給のための接続およびデータ伝送インターフエースとの接続がなされる。カード上のマイクロプロセッサはそのＲＯＳに記憶された制御プログラムで制御される。ユーザの識別子および発行者の識別子もまた他の情報と共にＲＯＳに記憶されている。

このようなマイクロプロセッサを含むカードの例は英国特許出願第２０８１６４４Ａ号および第２０９５１７５Ａ号にある。

欧州特許出願第８２３０６９８９３号はＰＩＮがネットワークを介して間接的に伝送されるようなＥＦＴネットワークの取引き端末から入力されたＰＩＮの有効性を検査するための方法および装置について記載するものである。ＰＩＮおよびＰＡＮを用いて許可パラメータ（ＤＡＰ）を導出する。一意的なメッセージをＰＡＮと共にホストプロセッサに送り、そこでそのＰＡＮを用いて有効な許可パラメータ（ＶＡＰ）を識別する。このＶＡＰを用いてメッセージをコード化し、その結果（メッセージ確認コード：ＭＡＣ）を取引き端末に返す。端末はＤＡＰを用いて同時に導出メッセージ確認コード（ＤＭＡＣ）を生成し、そのメッセージをコード化する。そうしてＤＭＡＣとＭＡＣを比較し、その比較結果を用いてＰＩＮの有効性を判断する。

（12）

こうしたシステムではＤＡＰおよびＶＡＰの生成は短いＰＩＮだけに基づいて行われるので、暗号化に関して難点がある。その上、ＥＦＴ端末は識別カードで伝えられる情報の全てをアクセスしなければならず、システムの安全保護の点からいつても問題である。

各定義域がデータプロセッサを含み、暗号化によつて機密保持された伝送が行われるような多重定義域通信ネットワークでは、定義域間キーを設けねばならない。定義域間キーを設けてそれを使用するような通信安全保護システムは米国特許第４２２７２５３号に記載されている。ここに示される通信安全保護システムは各定義域がホストシステムと、それに関連するプログラムおよび通信端末の資源と、を有する多重定義域通信ネットワークの定義域間でデータを伝送するためのものである。ホストシステムおよび通信端末は複数のデータ安全保護装置を含む。データ安全保護装置は各々マスターキーを有する。これにより様々な暗号化オペレーションが可能となる。或る定義域のホストシステムが別の定義域のホストシステムと通信したいときは、両方のホストシステムで共通のセツションキーが設定され、暗号化オペレーションが可能となる。これは、両方のホストシステムでわかる互いに一致した定義域間キーを用いて達成される。しかしながら各ホストシステムは自身のマスターキーを相手側のホストシステムに明らかにする必要はない。定義域間キーは送信側のホストシステムにおいて１のキー（暗号化キー）の下で暗号化され、受信側のホストシステムにお

（13）

（14）

いては別のキー（別の暗号化キー）の下で暗号化される。送信側のホストシステムは暗号化されたセッションキーを生成して、送信側の定義域間キーの下で、セッションキーを再び暗号化し、これを相手のホストシステムに送信する。受信側のホストシステムは受信したセッションキーを定義域間キーの下での暗号から受信側のマスターキーの下での暗号に変換する（再暗号化する）。こうして両方のホストシステムで共通のセッションキーが使用できるようになるので、通信セッションが確立されて、これらのホストシステム間で暗号化オペレーションを進めることができる。

ホームバンキングシステムは顧客（ユーザ）の数が小規模である銀行のシステムとみなすことができる。システムのユーザには、たとえば、パーソナルコンピュータまたはキーボードを備えたテレビ受像機のような専用の端末装置が設置される。1組の装置が多数のユーザによつて共有されることもある。このシステムは個人的な情報へのアクセスの制御、一連の取引きの確認、およびそうした



た取引きの遂行の許可を保障するという安全保護上の要求を有する。

〔発明が解決しようとする問題点〕

以上説明したように従来技術におけるデータ通信システムは安全保護の点では未だ十分なものではない。

したがつて本発明の目的はデータ通信システムにおいてより優れた安全保護を提供することにある。

〔問題点を解決するための手段〕

本発明の目的は下記に示すセッション暗号キー更新方法を用いることによつて達成される。

ホストデータプロセッサが通信ネットワークを介して各々検証モジュールを含む複数のメッセージ起点ユニットに接続され、各検証モジュールごとに取引きセッションキーを発行し記憶し、ユーザの入力装置で記憶されるユーザ識別番号と、ユーザが別に記憶している秘密番号と、から導出さ



れるユーザ確認パラメータを各ユーザごとに発行し記憶するようなデータ通信システムにおいて、

(a) ユーザによつて取引きがメッセージ起点ユニットで開始されると、検証モジュールがユーザ識別番号と、現取引きセッションキーに基づくメッセージ確認コードと、を含む第1のメッセージを形成してホストデータプロセッサへ送るステップと、

(b) ホストデータプロセッサで第1のメッセージを受け取つてメッセージ確認コードを再生成し、これと受信したメッセージ確認コードとを比較するステップと、

(c) ランダムキーを生成するステップと、

(d) ランダムキー、ユーザ確認パラメータ、および現取引きセッションキーに基づき新たな取引きセッションキーを生成するステップと、

(e) 現取引きセッションキーを用いて暗号化されたユーザ確認パラメータと、ユーザ確認パラメータを用いて暗号化されたランダムキーと、を含む第2のメッセージを形成して検証モジュールへ送



るステップと、

(f) 検証モジュールでユーザの入力する秘密番号を受け取つてユーザ確認パラメータを再生成するステップと、

(g) 再生成されたユーザ確認パラメータと受信したユーザ確認パラメータとを比較してユーザの入力を検証し、これにより検証された正しいユーザ確認パラメータを用いてランダムキーを暗号解読し、ホストデータプロセッサに送られる次のメッセージのために使用される新たな取引きセッションキーを生成し記憶するステップと、

を有することを特徴とするセッション暗号キー更新方法。

〔実施例〕

本実施例はホームバンキングシステムで使用される安全保護技術に関する。公衆交換システム（ＰＳＳ）を介して顧客に接続される銀行のデータ処理センターは端末から受け取つたメッセージが有効な装置（銀行が許可した装置であつて、かつ、

そのユーザが有効なユーザである装置）から来たものであるかどうかを知る必要がある。

良好な実施例ではメッセージの起点ユニットとなる端末ごとに検証モジュールが存在する。検証モジュールは端末間で持ち運び可能である。各検証モジュールには検証モジュール識別子（ＶＭＩＤ）、シード番号（$VMSEED_n$）、初期取引きキー（$VMKEY_n$）、銀行識別アドレス（ＨＩＤＤ）およびインデックス番号（ＶＭＮＤＸ）が発行される。銀行はＶＭＩＤによつて指標付けされるこれら全てを記憶する。ユーザが取引きを開始すると、端末は$VMKEY_n$を用いて生成されたメッセージ確認コード（ＭＡＣ１）を含み、ＶＭＩＤおよびユーザ識別子ＵＩＤを有する第１のメッセージを構成する。

銀行は各ユーザに対してユーザ識別子（ＵＩＤ）およびユーザ秘密番号（ＵＰＷ）を有する。これらは他の適用例でいうとＰＡＮおよびＰＩＮと等価なものである。銀行のデータ処理センターは第１のメッセージを受け取ると、ＶＭＩＤを用いて



$VMKEY_n$の自身のバージョンを獲得して、ＭＡＣ１を再び生成する。こうして再生成されたＭＡＣ１と受信したＭＡＣ１とを比較する。このオペレーションが成功すると、ランダムキー（ＲＮＫＥＹ）が生成され、ＶＭＩＤと共にＲＮＫＥＹおよび$VMSEED_n$を用いて新しい取引きセッションキー（$VMKEY_{n+1}$）が生成される。ＲＮＫＥＹおよび$VMSEED_n$を用いて新しい$VMSEED_{n+1}$もまた生成される。

$VMSEED_n$および$VMKEY_n$を用いて暗号化された、ＵＩＤおよびＵＰＷに基づく確認パラメータ（ＵＶＰ）を含む第２のメッセージ（ＭＳＧ２）が生成される。これをＵＡＰ（ユーザ確認パラメータ）と呼ぶ。このメッセージはＵＶＰ、$VMSEED_n$、およびＶＭＩＤを用いて暗号化されたＲＮＫＥＹも含む。

端末がＭＳＧ２を受け取つて、ユーザがＵＰＷ（ＰＩＮ）を入力すると、端末はＵＶＰを再び生成して、これと受信され暗号解読されたＵＶＰとを比較する。端末はそれからＲＮＫＥＹを暗号解



読し$VMKEY_{n+1}$および$VMSEED_{n+1}$の自身バージョンを再び生成することができる。こうして新しい取引きセッションキー（$VMKEY_{n+1}$）とシード（$VMSEED_{n+1}$）とを用いて端末から送られる次のメッセージを確認する。

このシステムを用いるならば部外者は検証モジュールをエミュレートすることはできない。すなわち検証モジュールの処理のたびごとに重要なパラメータ（ＶＭＫＥＹおよびＶＭＳＥＥＤ）を更新できるような銀行を装うことはできない。したがつて優れた安全保護システムを提供することができる。

本発明は１つのメッセージの転送のためにだけ用いられるキーの下で暗号化された確認パラメータ（ＵＶＰ）自身を利用することによつて、安全保護上、セッションキーを更新する、各検証モジュールの有効性を確認する、ホストの有効性を確認する、という特徴を含む。

第１図を参照してホームバンキングシステムの



概略を説明する。

銀行および同様な金融機関のホストプロセッサ１０は適切なインターフエースを介して公衆パケット交換網（ＰＳＳ）１２のような通信媒体に接続される。このシステムのユーザ（顧客）は端末機１４を介してＰＳＳ１２と対話する（端末機１４はＰＳＳ１２に接続される）。

端末機１４はパーソナルコンピュータ、ビデオテックスシステムとして使用されるようなキーボード付テレビ受像機、または他の適切な入／出力表示装置でもよい。端末機１４はモデムを介してＰＳＳ１２に直接接続してもよいし、第１図に示すような局所ノード１６を介してＰＳＳ１２に接続してもよい。本発明を利用するホームバンキングシステムの各端末機は検証モジュール（ＶＡＬＭＯＤ）と相互接続できる。

検証モジュールは、知能機密保護カード、携帯用ＰＩＮＰＡＤ、完全な端末機、または端末機に設けられた論理モジュールを含む様々な物理装置の１つである。

第２図は良好な実施例で使用されるホストプロセッサ１０の構成を示す図である。ホストプロセッサ１０は制御ユニット２０を有する。制御ユニット２０はオペレーション制御用のマイクロコードを含む。記憶部２１は送受モジュール２２に接続される。記憶部１２は外部ディスク記憶装置またはその他同様な装置でもよい。送受モジュール２２は、それ自身、通信媒体（第１図ではＰＳＳ１２）に接続されたモデムを含んでいてもよい。確認メッセージ生成器２３、ランダム番号生成器２４、取引きキー生成器２５、メッセージ構成レジスタ２６、および暗号化／暗号解読（Ｅ／Ｄ）ユニット２７は共通のバスを介して記憶部２１および制御ユニット２０へ接続される。入力メッセージは記憶部２１へ直接に経路指定され、出力メッセージはメッセージ構成レジスタ２６から直接に送信されるかまたは記憶部２１を介して送信される。

もちろん多重プロセッサにおいては、第２図に示すユニットは、制御プログラムがオペレーティ



ングシステムの優先度に応じてタスクをレジスタおよび処理ユニットに割り振るようにする限りは、個別に識別可能でなくてもよい。

第３図は検証モジュール１４の構成を示す図である。検証モジュール１４はマイクロプロセッサ３０、ＲＡＭ３１、ＲＯＭ３２を含む。ＲＯＭ３２は検証モジュールおよび暗号化／暗号解読（Ｅ／Ｄ）ユニット３３のための制御用マイクロコードを有する。共通のバスが以上の各ユニットを送受ユニット３４に接続する。メッセージは送受ユニット３４へ送られる前に初めに生成されＲＡＭ３１に記憶される。受信メッセージはユニットがそれに作用する前に記憶される。

検証モジュールそれ自体は第３図に示す構成要素を全て含んでいる必要はない。たとえば送受ユニット３４およびマイクロプロセッサ３０は、取引きの行われる、その検証モジュールに接続される端末機のユニットであつてもよい。

次にこのシステムの動作について説明する。銀行または金融機関は顧客（または顧客がその特定



の発行者のシステム、たとえば銀行の支店、と対話したいときにそれができるような場所）に検証モジュール（ＶＡＬＭＯＤ）を発行する。したがつてＶＡＬＭＯＤは多数の顧客で共有できる（異なる場所を移動できる）。顧客は金融機関によつて発行されるどのモジュールでも使用可能である。その機関のホストシステムのところのデータをアクセスする必要のある顧客にはユーザ識別番号（ＵＩＤ）およびユーザ用の秘密の合言葉（ＵＰＷ）が与えられる。その顧客は必ずその機関によつて発行された検証モジュールを使用しなければならない。銀行の場合は、ＵＩＤは個人会計番号（ＰＡＮ）と等価でありＵＰＷは個人識別番号（ＰＩＮ）と等価である。

検証モジュールの発行

ＶＡＬＭＯＤは下記の情報を記憶する。

(a) ＶＡＬＭＯＤ識別子（ＶＭＩＤ）

(b) 秘密の１６進データ値（$VMSEED_n$）

(c) 秘密の暗号キー（$VMKEY_n$）



(d) ゼロにセットされたインデックス番号（ＶＭＮＤＸ＝ｎ）

(e) ユーザのホストの識別子（ＨＩＩＤ）、これはたとえばＰＳＳのユーザアドレスである。

以上の情報はＶＭＩＤで指標付けられるホスト側にも記憶されている。$VMEED_n$は、通常、データ暗号キーＤＫＥＹの下で$E_{DKEY}$（$VMSEED_n$）の形に暗号化することによつてホスト側で保護される。$VMKEY_n$はホスト側でホストマスターキーの下で$E_{HMKO}$（$VMKEY_n$）の形に暗号化され記憶される。

ＵＩＤはその機関によつて決定されユーザデータバンクへのインデックスとして働く。ＵＰＷはその特定のＵＩＤと共に用いる、機関によつて生成されるランダムな値である。ＵＩＤおよびＵＰＷは各ユーザへ内密に供給される。この２つの値を組み合せて８つの１６進バイトから成るユーザ確認パラメータ（ＵＶＰ）を構成する。この組合せの形式は、情報が失われない限りは、重要ではなく、その機能は要求に応じて造り替えることが

できる。UVPは$E_{HMKO}$（UVP）の形で暗号キーとしてホスト側に記憶され、UIDにより指領される。

システムの使用法

1. ユーザはVALMODのある所へ行き自身のUIDを与えて（たとえば磁気ストライプカードまたはキーボードを介して）、VALMODはこのUIDを記憶する。
2. VALMODはHIID、VMID、VMPAR（VMNDXのパリティに応じて0または1の値をとる）、およびUIDを有するMSG1を含むメッセージをコンパイルする。
3. VALMODは$VMKEY_n$を用いてMSG1のためのメッセージ確認コードMAC1を生成する。
4. MSG1、MAC1が発行者に送られる。
5. VMNDXのパリティが正しければ、発行者は受信したMSG1および記憶された$VMKEY_n$を用いて（さもなければ前の値$VMKEY_{n-1}$



およびVMSEED$_{n-1}$を用いて）。参照となるMAC1を生成する。こうして生成したMAC1が受信したMAC1と同じでないときは、取引きは打ち切られる。
6. MAC1が有効ならば発行者はUIDを検査し、この検査が有効ならば発行者は暗号キーRNKEYをランダムに生成する。

a) $VMSEED_{n+1}=E_{RNKEY}(VMSEED_n)$
b) $VMKEY_{n+1}=D_{RNKEY}(VMSEED_n+VMID)$
c) $UAP=E_{VMKEY_n}(E_{UVP}(VMSEED_n))$
d) $UAKEY=E_{VMKEY_n}(E_{UVP}(VMSEED_n+VMID))$
e) $NEWKEY=E_{UAKEY}(RNKEY)$

発行者はa)およびb)を記憶し、d)を除く。
7. 発行者はUAPおよびNEWKEYを含むメッセージMSG2をコンパイルし、$VMKEY_n$を用いてMSG2のためのメッセージ確認コード



MAC2を付加する。
8. 発行者はMSG2およびMAC2をVALMODに送る。VALMODは記憶された$VMKEY_n$を用いてMAC2を検証する。MAC2が不当なものであれば取引きは打ち切られる。
9. VALMODはユーザのUPWを要求する。このUPWと記憶されたUIDとを組み合せて検証されるべきUVPを生成する。
10. VALMODは6cに示すようにUVPおよび記憶された$VMKEY_n$を用いて参照となるUAPを生成する。このUAPが受信したUAPと同じでないときは、取引きは打ち切られる。
11. VALMODは6dに示すように検証されたUVPおよび記憶されたVMSEED$_n$を用いてUAKEYを生成する。VALMODはUAKEYを用いて受信したNEWKEYを暗号解読してRNKEYを得る。
12. VALMODは6aおよび6bに示すように記憶されたVMSEED$_n$および受信したRNKEYを用いてVMSEED$_{n+1}$および$VMKEY_{n+1}$を生成する。VMSEED$_{n+1}$および$VMKEY_{n+1}$はVMSEED$_n$および$VMKEY_n$の代わりにVALMODに置かれ、VMNDXが1だけ増分される。
13. VALMODはMSG1の内容を含む確認メッセージMSG3を生成し、$VMKEY_{n+1}$を用いてMSG3のためのメッセージ確認コードMAC3を付加する。これが発行者に送られる。
14. 発行者はこれを受け取ると$VMKEY_{n+1}$を用いてMAC3を検証する。MAC3が不当なものであれば取引きは打ち切られ、VALMODは同期外れが通告される（再発行されるまではそれを使用することができない）。
15. 発行者は適切なキーの下で暗号化されたVMSEED$_{n+1}$および$VMKEY_{n+1}$でVMSEED$_n$および$VMKEY_n$を置き換える。

以上に示したオペレーションから言えることは、VALMODは下記の条件の場合にのみ秘密のデータを発行者と同期して変更するということである。

a) ＶＡＬＭＯＤは有効であつて既に同期化されている。

b) ユーザは有効かつ確認されている。

これらの条件を満たすことについての吟味はＭＡＣ３を用いて行われる。

ＶＡＬＭＯＤおよび発行者の間でメッセージを記録するので、部外者はＶＡＬＭＯＤをエミュレートすることはできない。すなわち部外者は、ＶＡＬＭＯＤを扱うたびに重要なパラメータ（ＶＭＳＥＥＤおよびＶＭＫＥＹ）を更新するような発行者を装うことはできない。したがつて優れた安全保護システムが提供される。

ＭＳＧ３を受け取ることによつてユーザデータおよび機構を正当に所有するユーザに、ユーザ自身の端末機を介して発行者ホストからアクセスできるようになる。一連の為替取引きは端末のユーザによつて遂行され検査される。この通信は$VMKEY_{n+1}$を用いてＭＡＣ３を生成することによつて確認される。

所望の全ての作業が完了するときに、為替取引



きを行う顧客の承認を得る必要がある。これは"完了"メッセージを発行者に送ることによつてなされる。こうしてＰＩＮ（ＵＰＷ）の再エントリを含む別のＶＡＬＭＯＤシーケンスが繰り返される。

$VMKEY_{n+2}$（新たに承諾されたもの）を用いて確認されたＭＳＧ３を受け取るのは、処理する発行者の権限である。$VMKEY_{n+3}$でこれが確認され、その肯定応答がユーザの端末機に返される。

下記に示す表は取引きセッションのオペレーションの間、および検証に関するメッセージ（ＭＳＧ１、ＭＳＧ２、およびＭＳＧ３）の形成の間に、ＶＡＬＭＯＤ側およびホストプロセッサ側で記憶され生成される項目を示すことによつて、これまでに説明した手法を簡略的に表わすものである。



ＶＡＬＭＯＤ側

記憶されるもの

- ＶＭＩＤ
- $VMSEED_n$
- $VMKEY_n$
- ＶＭＮＤＸ
- ＨＩＩＤ
- ＨＩＩＤ

入力されるもの

- ＵＩＤ

ＨＩＩＤ、ＶＭＩＤ、ＶＭＰＡＲ（ＶＭＮＤＸに基づく）、ＵＩＤ、および$MAC1$（$VMKEY_n$に基づく）を含むＭＳＧ１がＶＡＬＭＯＤからホストへ送られる。



ホスト側

記憶されるもの

- ＶＭＩＤ
- $VMSEED_n$
- $VMKEY_n$
- ＶＭＮＤＸ
- ＵＩＤ
- ＵＶＰ

生成されるもの

- ＭＡＣ１
- ＲＮＫＥＹ
- $VMSEED_{n+1}$
- $VMKEY_{n+1}$
- ＵＡＰ
- ＵＡＫＥＹ

ＶＭＩＤ、ＵＡＰ（$VMSEED_n$（ＵＶＰ）、$VMKEY_n$に基づく）、ＮＥＷＫＥＹ（ＲＮＫＥＹ、ＵＡＫＥＹに基づく）、および$MAC2$（$VMKEY_n$に基づく）を含むＭＳＧ２がホストからＶＡＬＭＯＤへ送られる。

入力されたＵＰＷより

生成されるもの

- ＵＶＰ
- ＵＡＰ
- ＵＡＫＥＹ
- ＲＮＫＥＹ
- $VMSEED_{n+1}$
- $VMKEY_{n+1}$

ＨＩＩＤ、ＶＭＩＤ、ＶＭＰＡＲ、ＵＩＤ、およびＭＡＣ３（$VMKEY_{n+1}$に基づく）を含むＭＳＧ３がＶＡＬＭＯＤからホストへ送られる。

ＶＡＬＭＯＤおよびホストはいずれも$VMSEED_{n+1}$および$VMKEY_{n+1}$を記憶する。

どの段階においてもＶＡＬＭＯＤおよびホストの部外者が利用できる$VMSEED_{n+1}$および$VMKEY_{n+1}$は存在しない。

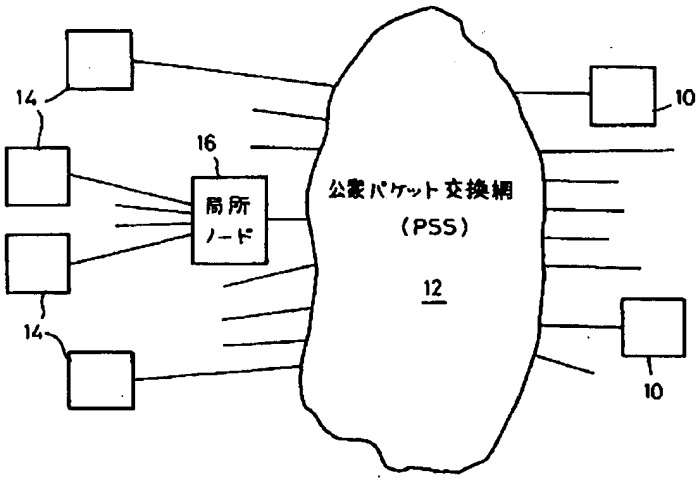
〔発明の効果〕

以上説明したように本発明によれば、メッセージ交換のたびごとに自動的にキーの更新がなされるので、従来に比べてより優れた安全保護システムが提供される。

4.図面の簡単な説明

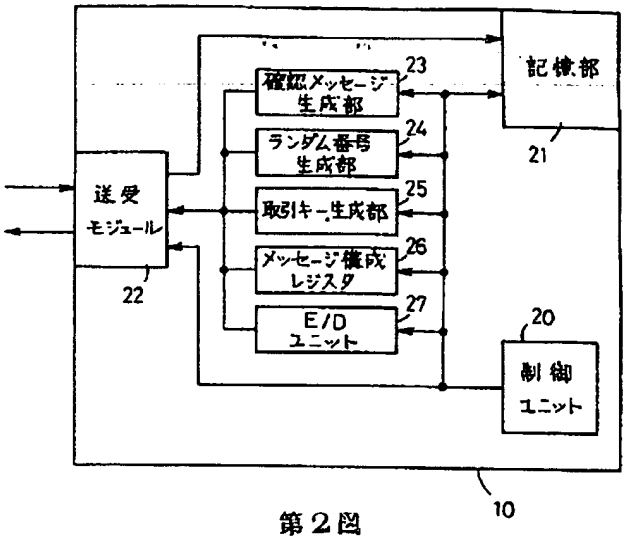
第１図はホームバンキングデータ通信システムを簡略的に示すブロック図、第２図はホストプロセッサの構成例を示すブロック図、第３図は検証モジュールの構成例を示すブロック図である。



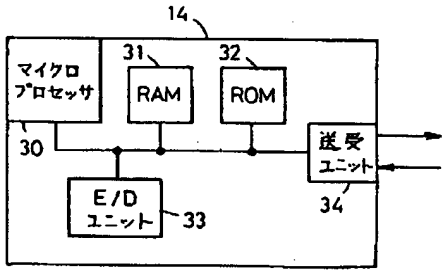



10 … ホストプロセッサ
14 … 端末機

第１図


記憶部
21
確認メッセージ生成部
23
ランダム番号生成部
24
取引キー生成部
25
メッセージ構成レジスタ
26
E/Dユニット
27
送受モジュール
22
制御ユニット
20
10

第２図


14
マイクロプロセッサ
30
31
RAM
32
ROM
送受ユニット
34
E/Dユニット
33

第３図